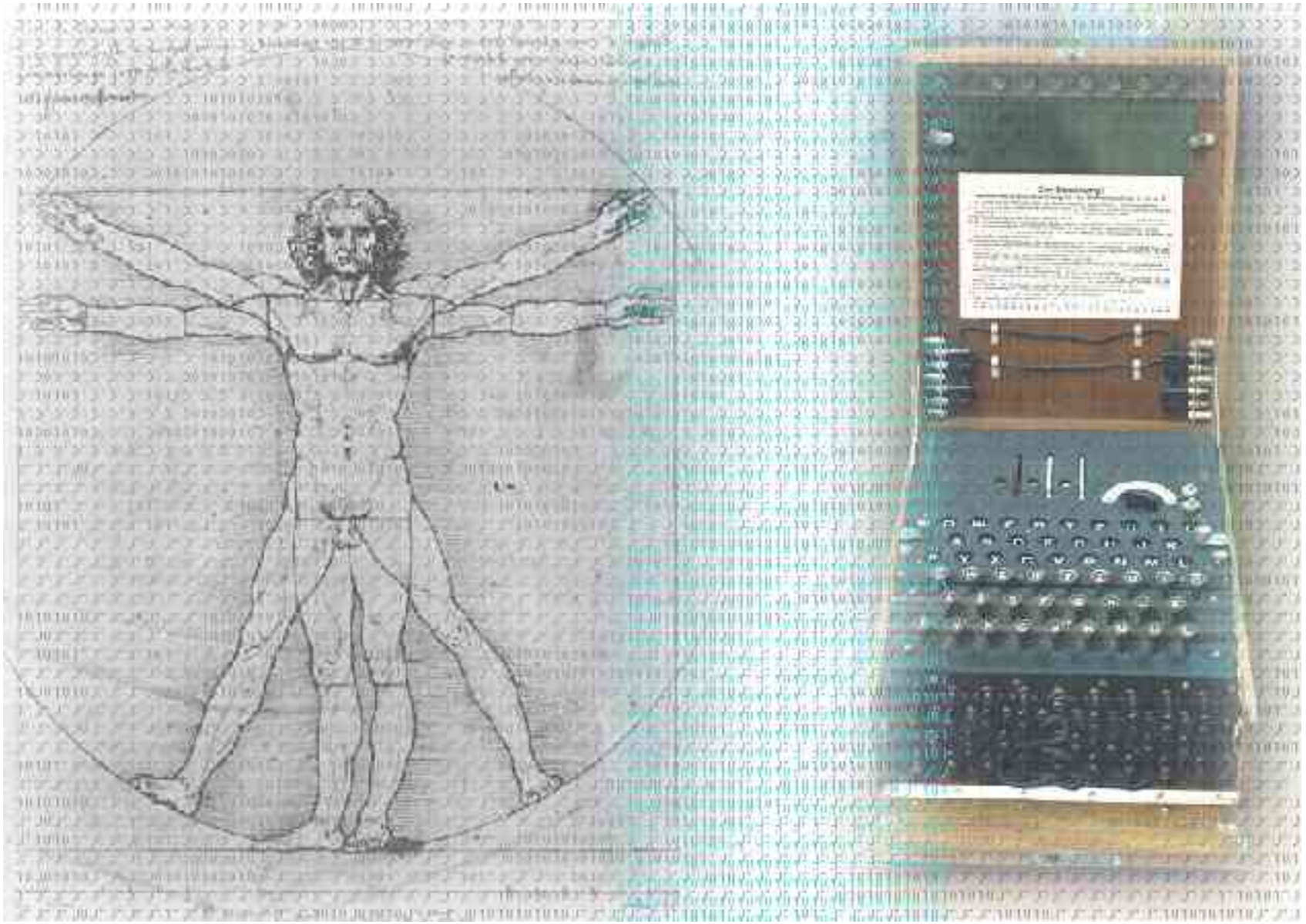
# Kryptographie



# Übersicht

- Klassische Verfahren
- Etwas Theorie
- Moderne symmetrische Chiffren
- AES-Entscheidung
- Die Kunst der Anwendung
- Fazit

# Klassische Verfahren

- Skytala: Vor rund 2.500 Jahren von den Griechen verwendet

- Papyrusstreifen um Holzstab wickeln
- „Schlüssel“ = Durchmesser des Stabes

# Klassische Verfahren

- Klartext: „Dies ist ein Test für die Skytala“


- Chiffrat: „defs iiük enry s t tda ieil ssea tt “

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| D | I | E | S | | I | S | T |
| E | I | N | | T | E | S | T |
| F | Ü | R | | D | I | E | |
| S | K | Y | T | A | L | A | |

**➔Transpositions-Chiffre**

# Klassische Verfahren

- Cäsar-Chiffre:Verschieben des Alphabets
- „Schlüssel“ = Offset

| A | B | C | D | E | F | G | ... | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C | D | E | F | G | H | I | ... | U | V | W | X | Y | Z | A | B |

- Klartext: Hallo
- Chiffrat: Jcnnq

➔**Substitutions-Chiffre (monoalphabetisch)**

# Klassische Verfahren

- Vigenère-Chiffre: Mehrere Cäsar-Chiffren hintereinander
- Je länger der Schlüssel, desto besser

| K | R | Y | P | T | O | G | R | A | P | H | I | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C | O | D | E | C | O | D | E | C | O | D | E | C |
| M | F | B | T | V | C | J | V | C | D | K | M | G |

**➔Substitutions-Chiffre (polyalphabetisch)**

# Klassische Verfahren

- Enigma: Polyalphabetische Chiffre
- Neu: Langer Schlüssel durch 3 Rotoren (Periode = 17576)
- Mehrere Rotoren zur Auswahl
- Steckbrett für weitere Permutation

# Klassische Verfahren

- Rotor: Permutation durch interne Verdrahtung
- Rotoren bewegen sich bei jedem Tastendruck weiter (wie Kilometerzähler)

- Schlüssel: Auswahl der Rotoren, Steckbrett
- Anfangsstellung der Rotoren: Zu Beginn des Funkspruchs mit Tagesschlüssel verschlüsselt

# Etwas Theorie...

Aufbau und Klassifizierung

- Grundelemente: Substitution und Transposition
- Stromchiffren / Blockchiffren:
  - Stromchiffren verarbeiten Klartext Zeichen für Zeichen (typisch: Zufallsbit XOR Klartextbit)
  - Blockchiffren: Ganze Klartextblöcke werden auf einmal bearbeitet

# Etwas Theorie...

Modi von Blockchiffren

- ECB (Electronic codebook)
  - Jeder Block wird separat verschlüsselt
  - Kein Problem beim Verlust eines Blocks
  - Jeder Block kann separat angegriffen werden
- CBC (Cipher block chaining)
  - Verschlüsselt wird Klartext XOR vorheriges Chiffrat
  - Effektive Verkettung ganzer Blöcke

# Etwas Theorie...

- CFB (Cipher feedback)
  - Der vorherige Ausgabeblock wird verschlüsselt und mit den aktuellen Daten geXORt.
  - Vorteil: Übertragung einzelner Bytes möglich.
- OFB (Output feedback)
  - Ein Startwert wird immer wieder verschlüsselt
  - Dieser Pseudo-Zufallsstream wird mit dem Klartext geXORt.
  - Vorteil: Vorausberechnung möglich.

# Etwas Theorie...

Angriffsarten

- Brute force
- Known plaintext
- Chosen plaintext
- Differenzielle Kryptanalyse
- Lineare Kryptanalyse
- Timing / Power attacks, Tampering attacks
- ...und weitere esoterische Angriffe

# Etwas Theorie...

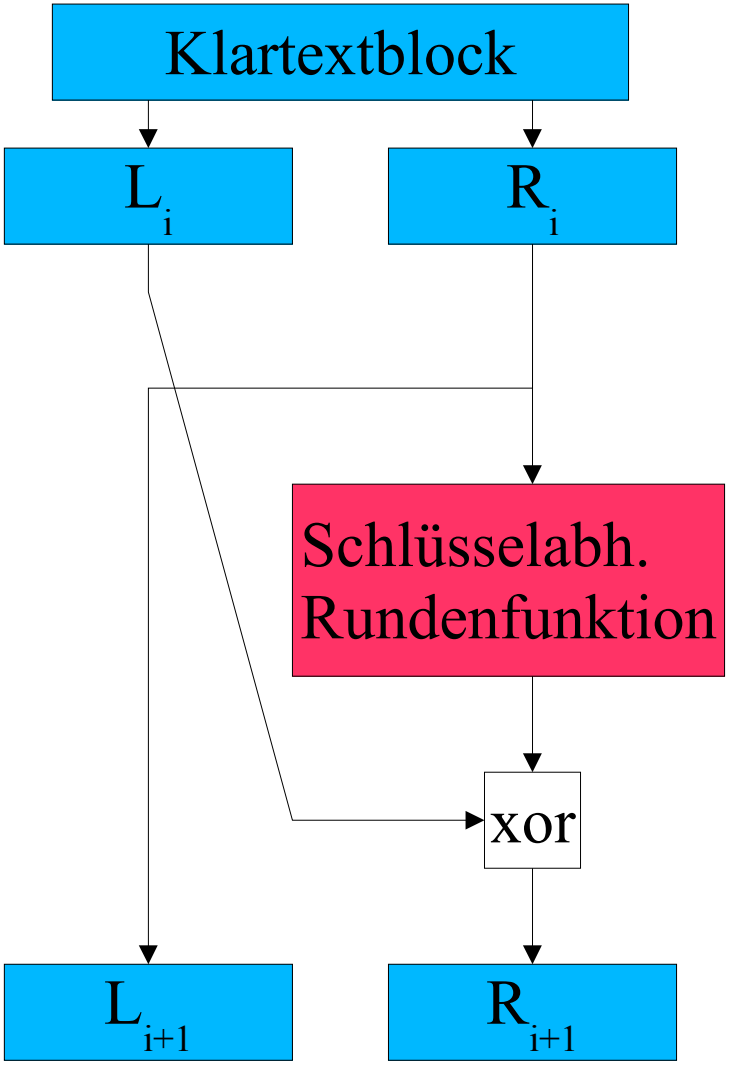
Definition von Sicherheit

- Computational security
  - Bester bekannter Angriff zu langsam für praktischen Nutzen / langsamer als brute force attack
  - Nicht beweisbare Definition
- Absolute security
  - Chiffre nicht zu brechen, egal wie hoch der Aufwand
  - Nach Shannon: $P(p|c) = P(p)$
  - Bisher nur für Vernam-Chiffre nachweisbar

# Moderne symmetrische Chiffren

Produktchiffren

- Einzelne, relativ einfache Schritte
- Mehrfache bzw. wiederholte Anwendung
- Spezialfall: Feistel-Netz
  - Rundenfunkion muß nicht invertierbar sein



# Moderne symmetrische Chiffren

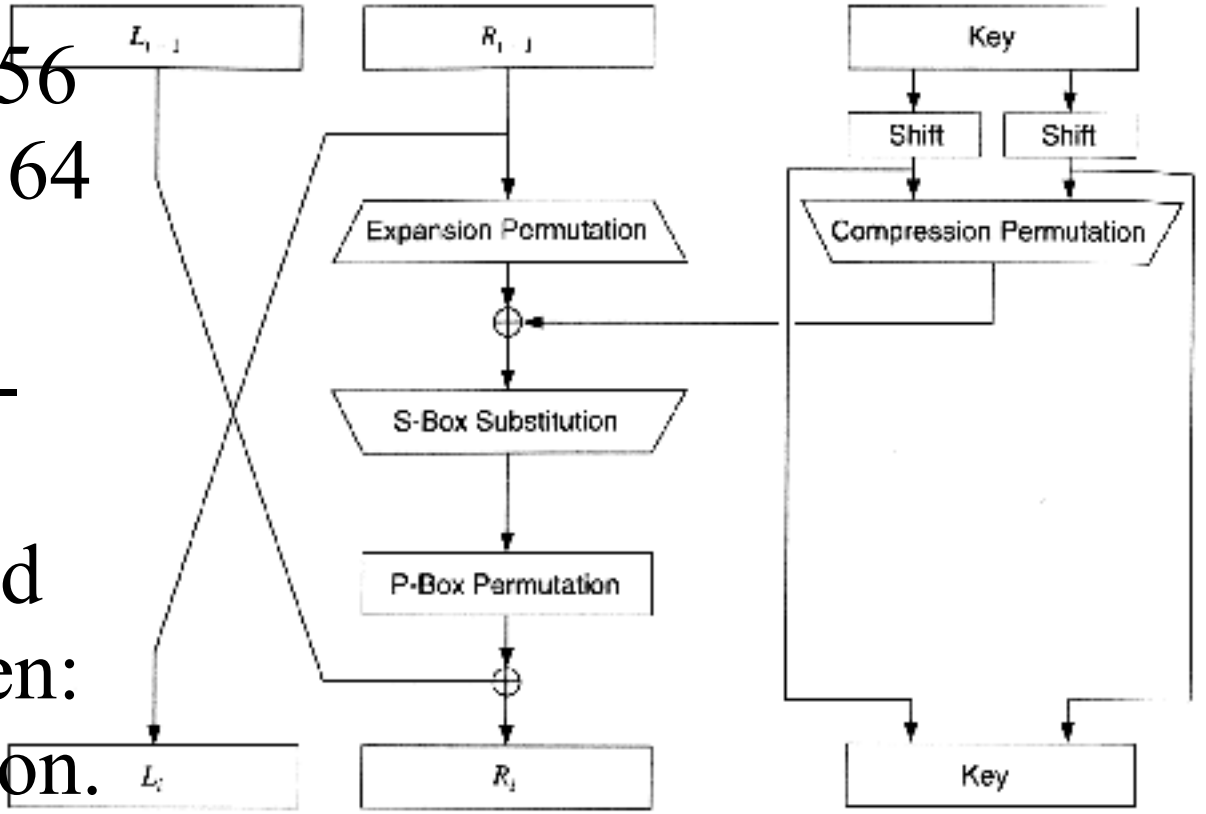
Der Klassiker: DES

- Erster Standardalgorithmus (1974)
- Algorithmus wurde von der NSA evaluiert
  - Schlüssellänge von 128 bit auf 56 bit reduziert
  - S-Boxen ohne Erklärung verändert
- 1990: Biham und Shamir entdecken differenzielle Kryptanalyse. Daraufhin werden die Design-kriterien von DES veröffentlicht.

# Moderne symmetrische Chiffren

Der Klassiker: DES

- Schlüssellänge 56 bit, Blocklänge 64 bit.
- Aufbau: Feistel-Netz mit 16 Runden. Vor und nach den Runden: Feste Permutation.



# Moderne symmetrische Chiffren

Kritik an DES

- Verdacht der Einbau einer Hintertür durch die NSA konnte nie ganz ausgeräumt werden
- Zu geringe Schlüssellänge (Übergangslösung: 3DES mit 112 bzw. 168 bits)
- Softwareimplementierungen langsam

# Moderne symmetrische Chiffren

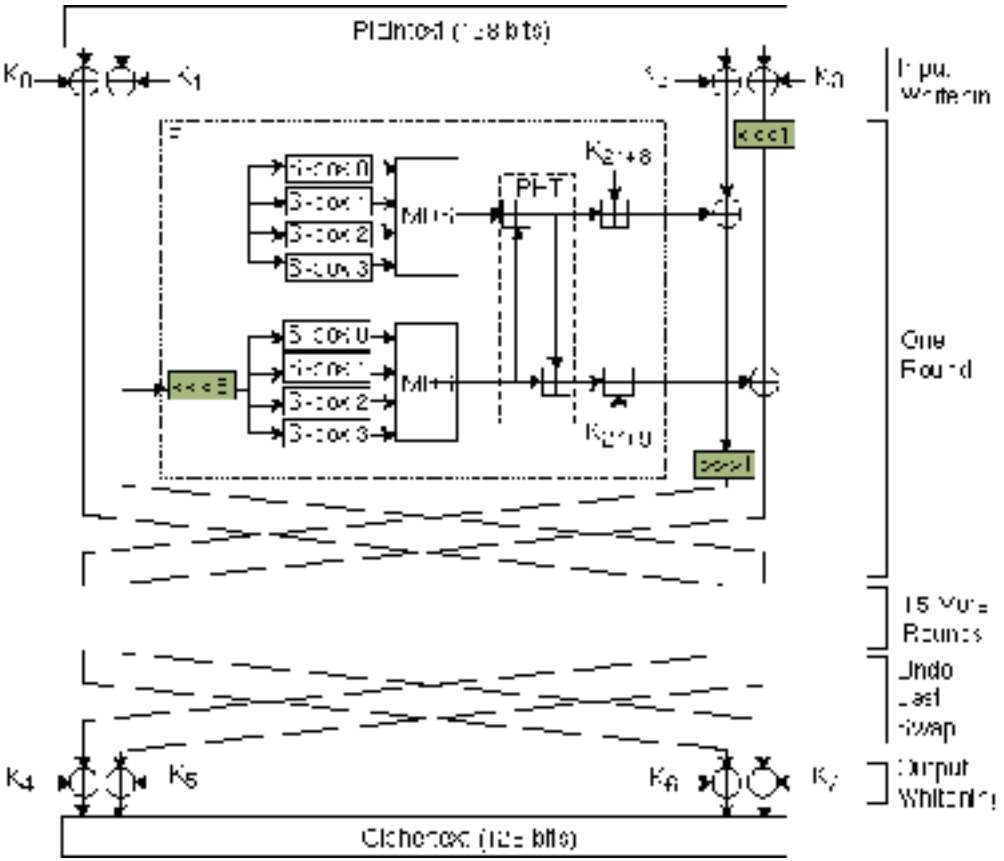
Die „Volkschiffre“: Twofish

- Entworfen vom Team von Bruce Schneier
- Feistel-Netz (leicht variiert) mit 16 Runden, Pre- und Post-Whitening (schlüsselabhängiger Schritt)
- 128 bit Blockgröße
- Schlüssellänge 128, 192 oder 256 bit

# Moderne symmetrische Chiffren

Verwendete Elemente:

- Schlüsselabhänige S-Boxen
- Diffusion (Verteilung der Redundanzen):
  - MDS-Matrizen (Maximum Distance Separable code)
  - Pseudo-Hadamard-Funktion



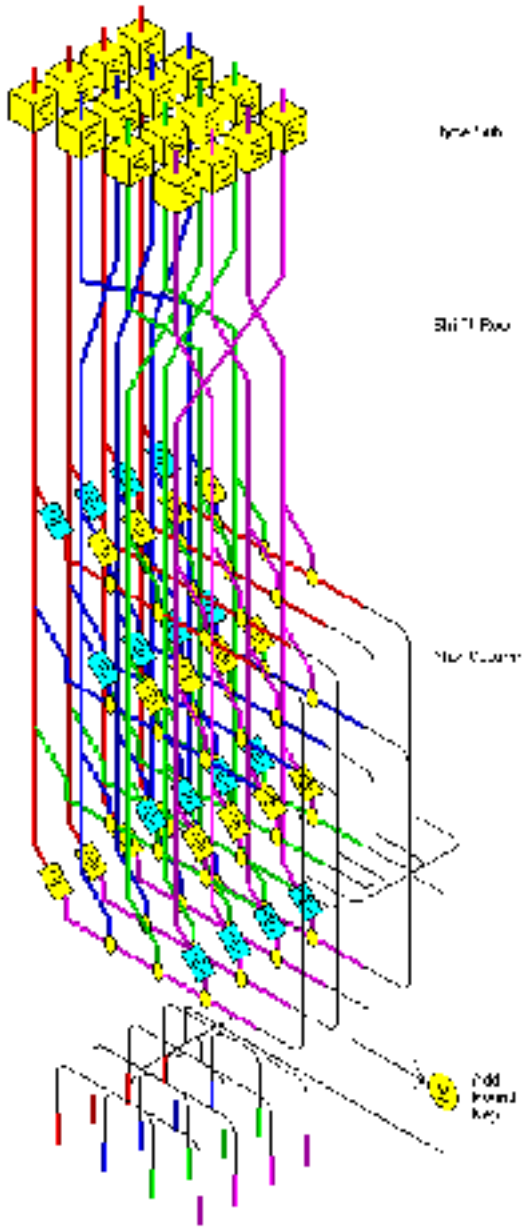
# Moderne symmetrische Chiffren

AES, der „neue DES“: Rijndael

- Entwickelt von J. Daemen und V. Rijmen
- 10-14 Runden einer invertierbaren Funktion
- Pre-Whitening, veränderte letzte Runde als Post-Whitening
- Rundenzahl abhängig von der Schlüssellänge
- Block- und Schlüssellänge (unabhängig voneinander) 128, 192 oder 256 bits.

# Moderne symmetrische Chiffren

- Ablauf
  - Key expansion
  - AddRoundKey
  - n * Round
  - FinalRound
- Round / FinalRound
  - ByteSub
  - ShiftRow
  - MixColumn (bei Round)
  - AddRoundKey



# Moderne symmetrische Chiffren

Aufbau Rijndael

- Anordnung des Klarextbocks in eine 4xN-Matrix
- ByteSub: Statische S-Box, für jedes Byte einzeln
- ShiftRow: Rotiert Zeilen byteweise
- MixColumn: Matrixmultiplikation (statisch)
- AddRoundKey: Byteweises XOR
- Pre-Whitening mittels AddRoundKey
- Key expansion benutzt auch S-Box

# Moderne symmetrische Chiffren

Der AES-Entscheidungsprozeß

- DES nicht mehr hinreichend sicher
- Erste Ausschreibung im Januar '97
- Voraussetzungen:
  - Blockchiffre, Blockgröße 128 bit
  - Schlüssellängen 128, 192 und 256 bit
  - Unclassified, öffentlich verfügbar
  - Keine Patentansprüche, kostenlose Nutzung weltweit

# Moderne symmetrische Chiffren

- August '98: Veröffentlichung von 15 Kandidaten
- 1 Jahr für public comments, Analysen, etc.
- August '99: Veröffentlichung der Finalisten
  - MARS (IBM)
  - RC6 (RSA Labs)
  - Rijndael (Daemen, Rijmen)
  - Serpent (Anderson, Biham, Knudsen)
  - Twofish (Schneier, Kelsey, Ferguson, Whiting, Wagner)

# Moderne symmetrische Chiffren

Entscheidungskriterien

- Sicherheit
  - Resistenz gegen bekannte Angriffe, relative Sicherheit
  - Mathematische Basis
- Kosten
  - Keine Lizenzen
  - Geschwindigkeit, Speicherbedarf
- Charakteristiken des Algorithmus
  - Weitere Schlüssel- und Blockgrößen
  - Implementierbarkeit auf versch. Plattformen

# Moderne symmetrische Chiffren

Die Entscheidung

- Keiner der Finalisten wurde gebrochen
- Security margin: MARS, Serpent, Twofish: high, Rijndael, RC6 adequate.
- Vorteile von Rijndael: Einfach, geringer Speicherbedarf, sehr performant.
- Rijndael in jedem Test oberes Mittelfeld

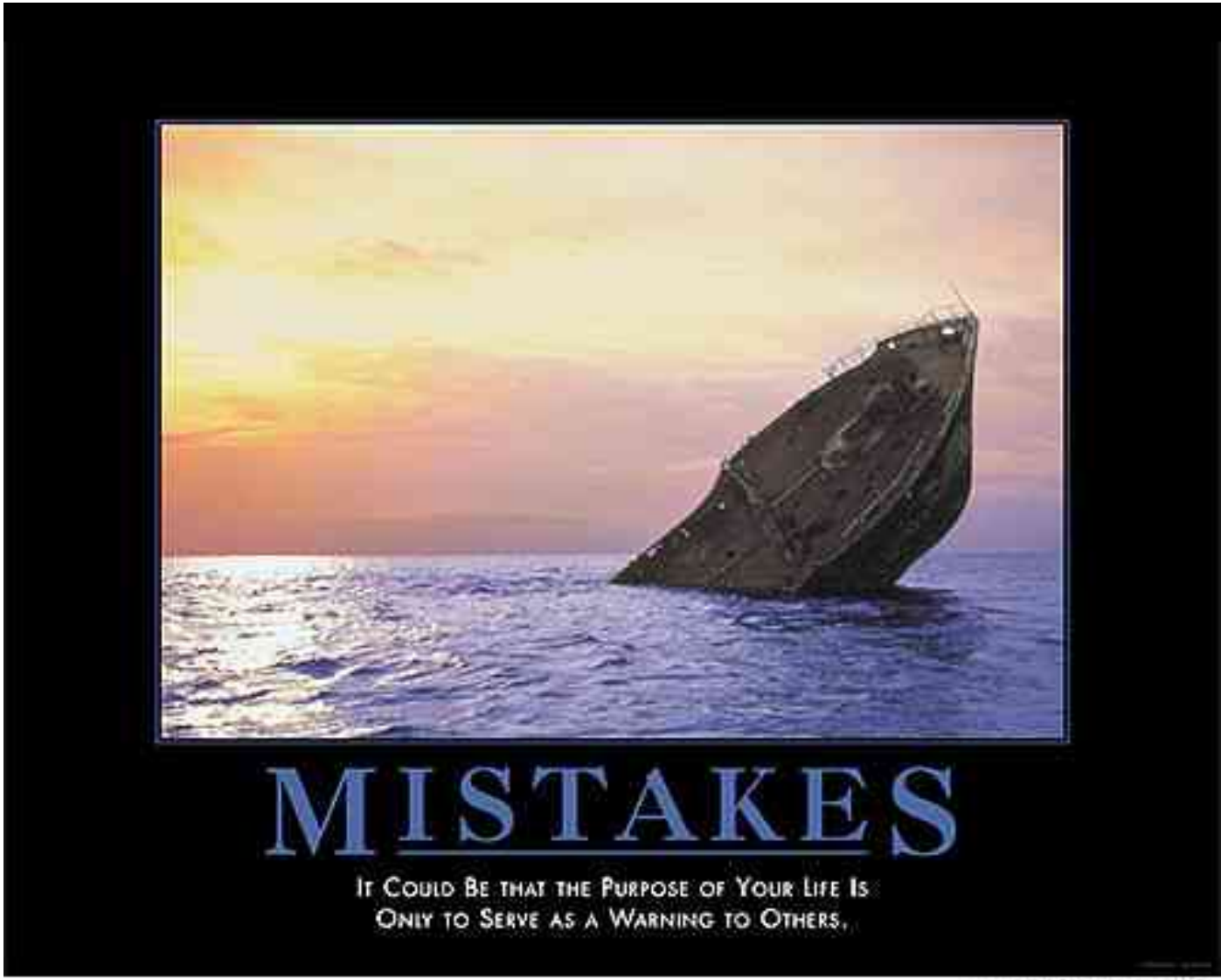
# Die Kunst der Anwendung

„Security is a process, not a product“

(B. Schneier)

- Kryptographie ist nicht alles
- Das schwächste Glied der Kette ist entscheidend
- Je komplexer ein System, desto leichter schleichen sich Fehler ein
- Todsünden: Überheblichkeit, Selbstsicherheit, Verschlossenheit

# Die Kunst der Anwendung



# Die Kunst der Anwendung

Netscape SSL security breach (Jan. '96)

- Verwendete Verfahren: RSA, RC4
- Session key: Zufallszahl (vom Browser)
- PRNG: rand_num=MD5(seed); seed++;
- seed=MD5(msec,pid+sec+(ppid<<12));
  - Account beim Ziel: Angriff trivial
  - Sonst: Zeit schätzbar/abfragbar. ppid oft 1. Shift um 12 bit nutzt nicht gesamten Zahlenbereich.

# Die Kunst der Anwendung

Microsofts PWL-Dateien (Dez. '95)

- „Paßwort-Safe“ für weitere Kennwörter
- RC4: Stromchiffre (PRNG xor Klartext), Schlüssellänge auf 32 bit(!) reduziert
- Ersten 20 Bytes: Username, gefüllt mit Nullen. Username = Dateiname.
- Jedes Kennwort wird mit dem selben PRNG-Stream verschlüsselt (RC4 jedes Mal neu initialisiert)

# Die Kunst der Anwendung

Win2k EFS (encrypted file system, Jan. 2001)

- Ziel: Schutz bei „stolen laptops“ und „unrestricted access“ (Zitat: www.microsoft.com/technet/win2000/win2ksrv/technote/nt5efs.asp)
- Jede Datei mit separatem Session key verschlüsselt. Verfahren: DES
- Bei einzelnen Dateien: Zur Bearbeitung wird unverschlüsselte Kopie im temp-Verz. angelegt
- Kopie wird nicht physikalisch gelöscht

# Die Kunst der Anwendung

Completely superfluous system

- Schutz von Bild- und Tondaten
- Jedes Medium mit eigenem Disc Key geschützt
- Schlüssellänge: 40 bits, Algorithmus proprietär
- Mit gespeichert: $E(K_d,K_d)$ zum Testen des Keys
  - Test ideal für brute force Angriff
  - Durch Schwächen in der Chiffre (zwei Schiebe-register): Reduzierung von $2^{40}$ auf $2^{25}$ Versuche

# Ausblick

Was noch nicht angesprochen wurde...

- Asymmetrische Chiffren
- Hashfunktionen und PRNGs
- Threshold-Verfahren
- Kryptographische Protokolle
- Kryptographie ohne Computer
  - Optische Kryptographie
  - Mit manuellen Hilfsmitteln wie z. B. Spielkarten

# Fazit

- Verschlüsselung ist für Sicherheit zwar nötig, aber längst nicht hinreichend
- Security through obscurity ist snake oil
- Sicherheit immer kritisch betrachten